General Description

Red Balloon Security's BITWISE is a user-friendly assurance tool tailored to provide cyber assurance reporting at JFAC Levels of Assurance (LOA) for Xilinx and Intel FPGA chips. The Xilinx variant covers four families across four generations: 6 series, 7 series, UltraScale, and UltraScale+. In contrast, the Intel version features Agilex7, Stratix10, and Cyclone10 GX. BITWISE offers a range of FPGA bitstream transformation and hardening techniques that are easily accessible to users, even those without prior experience with vendor tools. Additionally, it provides operators with crucial guidance to address risks associated with identified threats. BITWISE effectively detects and reports on Common Vulnerabilities and Exposures (CVE) that could jeopardize the security of FPGA bitstreams, generating a time-stamped report to validate FPGA designs. This tool is essential for verifying both newly developed designs and those already in deployed in the field. BITWISE is also utilized to validate vendor software.

Xilinx

6-series

- Spartan Compatible
- Virtex Compatible
- .bit file format
- Plaintext configuration
- Encryption AES CBC 256
- Re-encryption AES CBC 256
- JFAC LoA Reporting
- Warm Boot Register Hardening

7-series

- Spartan Compatible
- Virtex Compatible
- Kintex Compatible
- Artix Compatible
- .bit file format
- Plaintext configuration
- Encryption AES CBC 256
- Re-encryption AES CBC 256
- JFAC LoA Reporting
- Warm Boot Register Hardening

UltraScale

- Kintex Compatible
- Virtex Compatible
- .bit file format
- Plaintext configuration
- Encryption AES GCM 256
- Re-encryption AES GCM 256
- Re-encryption RSA-2048
- JFAC LoA Reporting
- Warm Boot Register Hardening

UltraScale+

- Kintex Compatible
- Virtex Compatible
- Artix Compatible
- .bit file format
- Plaintext configuration
- Encryption AES GCM 256
- Re-encryption AES GCM 256
- Re-encryption RSA-2048
- JFAC LoA Reporting
- Warm Boot Register Hardening

Intel

Agilex 7

- .rbf file compatible
- Plaintext configuration
- ECDSA 256/348
- AES-256
- Verify Authentication signatures
- Resign bitstream
- Cosign SDM Firmware
- Re-encrypt bitstream
- JFAC LoA Reporting

Stratix 10

- .rbf file compatible
- Plaintext configuration
- ECDSA 256/348
- AES-256
- Verify Authentication signatures
- Resign bitstream
- Cosign SDM Firmware
- Re-encrypt bitstream
- JFAC LoA Reporting

Cyclone 10 GX

- .jic file compatible
- Plaintext configuration
- AES-256
- Encrypt Plaintext to AES
- Re-encrypt bitstream
- JFAC LoA Reporting

Developed using a cutting-edge high-performance reverse engineering tool, Open Firmware Reverse Analysis Konsole OFRAK (OFRAK) a binary analysis and modification platform. This technology facilitates an FPGA bitstream assurance tool, significantly enhancing efficiency by minimizing engineering hours and providing a cost-effective approach to integrating FPGA assurance techniques into your team's strategy.

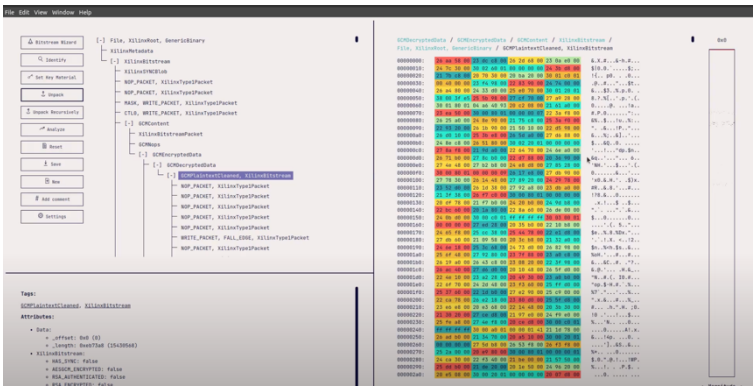
Xilinx Micro Bitstream

Bitwise introduces, for the first time, the Micro bitstream enhanced compression technology that was previously unveiled by the Naval Sea Systems Command (NAVSEA) Crane at GOMACTech 2023. This technology enables Xilinx users to compress bitstream configurations to the essential components required for programming an FPGA. Notably, Micro bitstream compression offers a significant advantage over the standard MFWR (Multiple Frame Write/Read) compression that is natively supported in Vivado, as it consistently achieves higher compression ratios. The implementation of Micro bitstream compression leads to substantial reductions in both file size and overall programming time, particularly beneficial for smaller RTL designs or scenarios involving partial reconfiguration. Additionally, Micro bitstreams are specifically supported for bitstreams generated with Per Frame CRC.

Xilinx Star Bleed Hardening

Xilinx 73541 - Design Advisory for 7 Series/Virtex-6 FPGAs: Addressing Bitstream Encryption outlines a successful exploitation of the insufficient error extension in AES-CBC mode, along with the execution of configuration commands, particularly WBSTAR, before authentication is completed. Bitwise can effectively mitigate attacks aimed at the Starbleed vulnerability through the following methods:

- shuffling configurations (randomizing the sequence of packets)
- inserting “no operation” (NOP) commands
- randomizing the NOP commands
- eliminating all write WBSTAR packets



This hardening process provides a minimum of 16 bits and can extend up to 27 bits of entropy. In this context, 2!" results in a very low probability of 1 in 134,217,728 for a successful attack, applicable only when NOPs are randomized.

Xilinx / INTEL Security Report

For security reporting, Bitwise automatically generates a report providing information to the end-user. In the security report for Xilinx, Bitwise details general metadata, details on the security, and configuration details. The general metadata displays design, part, and creation details. Design details explain the design name, whether it has been compressed, and the tool version that was used to design the bitstream. Part information will give the exact part number for the bitstream design. The configuration details in the report display packet types and a raw count of those packets in the configuration header of the bitstream. The Security report for INTEL Bitwise provides comprehensive metadata, including information on configuration, error detection through CRC, partial reconfiguration, security measures, anti-tamper features, the status of enabled or disabled security options, and any identified security vulnerabilities. Based on the security report, BITWISE recommends modifications to the bitstream. In the report, Bitwise can rapidly evaluate the bitstream's security posture according to the DoD's Level of Assurance (LoA) guidelines, stating the compliance-level for the target bitstream and providing actionable feedback that can be used to achieve compliance.

Xilinx / INTEL Time Stamp

For precise record-keeping, examining a bitstream from the design phase to its deployment in the field enables product developers and cybersecurity analysts to effectively analyze devices on-site. This process allows for the creation of detailed reports that identify any alterations in the security posture of the devices. Consequently, it ensures reliable accountability for the bitstreams utilized in essential devices.

Xilinx / INTEL Security Details

The Xilinx report outlines the encryption methodology and the particular encryption standard utilized in the design. It also specifies the storage location of the bitstream, indicating whether it will be housed in BBRAM or EFUSE. Furthermore, the report addresses the identification of key rolling. In the context of Xilinx devices, the presence of the WBSTAR write command signifies the components impacted by the Starbleed attack, thereby offering a prompt and precise evaluation of the device's security status.

The Intel report provides an overview of the JTAG status, specifying whether it is enabled or disabled and when the SDM is configured to use an internal oscillator. It further discusses the circumstances under which the key encryption update functions in force mode. Moreover, the report contains details about the virtual and lock eFuses, the HPS debug mode, and the initialization status of encryption in eFuses or BBRAM. Lastly, the security report indicates whether the Intrinsic ID PUF-wrapped encryption key in Quad SPI is currently activated.

Xilinx / INTEL Configuration Packet Overview

The configuration details offer valuable information specific to the devices. Xilinx showcases quantifiable results pertaining to Type 1 and Type 2 packets. In contrast, INTEL reveals the status of the active serial clock, the capability for remote system updates, and the presence of the HPS within the design.

Xilinx Type 1 Packet Breakdown

This pertains specifically to Xilinx components, where the bitstream can be analyzed to clearly identify the associated commands and the frequency of their execution through the evaluation of the bitstream.

Known Security Issues

By analyzing publicly accessible CVEs, BITWISE will indicate whether the bitstream is susceptible to any recognized vulnerabilities.

Security Score

A security score is provided to give a sense of how strong the devices security posture is after bitstream generation.

LoA 1 TD 6 Compliance Report

Bitwise focuses on the series released by the NSA regarding the protection of DoD microelectronics from adversarial influences, specifically addressing Level of Assurance 1 Threat Descriptor TD6. This report aims to enhance the security of FPGAs throughout their manufacturing, acquisition, programming, and initial integration phases. TD6 details strategies for mitigating risks associated with adversaries swapping configuration files on the target devices. The report specifies the necessary compliance measures:

- Incorporate cryptographic authentication of all loaded configuration data as part of the system containing the FPGA.
- Design the system to authenticate configuration data each time the data is loaded into the FPGA device.
- Configuration all production devices in a way that prevents direct read back of the private keys through electrical means.
- Use a NIST-approved algorithm and key length, as described in the latest approved version of FIPS 186, Digital Signature Standard, or FIPS 198, the Keyed-Hash Message Authentication Code (HMAC).
- Use security-evaluated authentication mechanisms.
- Disable operation or use of test access pins in fielded products.
- When the program selects mechanisms that allow application modifications, ensure authentication is enabled following the required NIST standards.
- Generate and store all authenticated keys on a program-controlled, FIPS 140-2 compliant, Level 2 Hardware Security Module (HSM).

It is essential to outline the required compliance measures, providing detailed information on whether compliance is achievable, not achievable, or cannot be assessed for the specific component. BITWISE will offer recommended actions to ensure compliance, thereby saving the design team significant time in meeting the LoA1 TD6 requirements and reducing the effort needed to determine compliance strategies. As the environment evolves and new CVEs emerge, BITWISE will be continuously updated to deliver critical information for achieving compliance.

Bitwise Xilinx Features

Item	Micro Bitstream	Star Bleed Hardening	Security Report	Time Stamp	Security Details	Configuration Packet Over View	Type 1 Packet Breakdown	Known Security Issues	Security Score	LoA 1 TD 6 Compliance Report
Spartan 6	x	x	✓	✓	✓	✓	✓	✓	✓	✓
Virtex 6	x	✓	✓	✓	✓	✓	✓	✓	✓	✓
Spartan 7	x	✓	✓	✓	✓	✓	✓	✓	✓	✓
Virtex 7	x	✓	✓	✓	✓	✓	✓	✓	✓	✓
Kintex 7	x	✓	✓	✓	✓	✓	✓	✓	✓	✓
Artix 7	x	✓	✓	✓	✓	✓	✓	✓	✓	✓
Kintex US	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Virtex US	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Kintex US+	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Virtex US+	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Artix US+	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

XILINX Product Table

Item	Product Table										
Spartan6 LX	XC6SLX4	XC6SLX9	XC6SLX16	XC6SLX25	XC6SLX45	XC6SLX75	XC6SLX100	XC6SLX150			
Spartan6 LXT	XC6SLX25T	XC6SLX45T	XC6SLX75T	XC6SLX100T	XC6SLX150T						
Virtex6 LXT	XC6VLX75T	XC6VLX130T	XC6VLX195T	XC6VLX240T	XC6VLX365T	XC6VLX550T	XC6VLX760				
Virtex6 HXT	XCE6VHX250T	XCE6VHX255T	XCE6VHX380T	XCE6VHX565T							
Virtex6 SXT	XC6VSX315T	XCE6VSX475T									
Spartan 7	XC7S6	XC7S15	XC7S25	XC7S50	XC7S75	XC7S100					
Virtex 7	XC7V585T	XC7V2000T	XC7VX330T	XC7VX415T	XC7VX485T	XC7VX550T	XC7VX690T	XC7VX980T	XC7VX1140T	XC7VH580T	XC7VH870T
Kintex 7	XC7K70T	XC7K160T	XC7K325T	XC7K355T	XC7K410T	XC7K420T	XC7K480T				
Artix 7	XC7A12T	XC7A15T	XC7A25T	XC7A35T	XC7A50T	XC7A75T	XC7A100T	XC7A200T	KU095	KU115	
Kintex US	KU025	KU035	KU040	KU060	KU085						
Virtex US	XCVU065	XCVU080	XCVU095	XCVU125	XCVU160	XCVU190	XCVU440				
Kintex US+	KU3P	KU5P	KU9P	KU11P	KU13P	KU15P	KU19P				
Virtex US+	VU3P	VU5P	VU7P	VU9P	VU11P	VU13P	VU19P	VU23P	VU27P	VU29P	
Virtex US+ HBM	VU31P	VU33P	VU35P	VU37P	VU45P	VU47P	VU57P				
Artix US+	AU7P	AU10P	AU15P	AU20P	AU25P						

Bitwise INTEL Features

Item	AES-256	ECDSA 256/348	Security Report	Time Stamp	Security Details	Configuration Packet Over View	Cosign SDM Firmware	Known Security Issues	Security Score	LoA 1 TD 6 Compliance Report
Agilex 7 F Series	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Agilex 7 I Series	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Agilex 7 M Series	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Stratix 10 GX	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Stratix 10 SX	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Stratix 10 TX	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Stratix 10 MX	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Stratix 10 DX	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Stratix 10 NX	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Stratix 10 AX	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cyclone 10 GX	✓	X	✓	✓	✓	✓	x	✓	✓	✓

INTEL Product Table

Item	Product Table										
Agilex 7 F Series	AGF 006	AGF 008	AGF 012	AGF 014	AGF 019	AGF 022	AGF 023	AGF 027			
Agilex 7 I Series	AGI 019	AGI 022	AGI 023	AGI 027	AGI 035	AGI 040	AGI 041				
Agilex 7 M Series	AGM 032	AGM 039									
Stratix 10 GX	GX 400	GX 650	GX 850	GX 1100	GX 1650	GX 2100	GX 2500	GX 2800	GX 1660	GX 2110	GX10M
Stratix 10 SX	SX 400	SX 650	SX 850	SX 1100	SX 1650	SX 2100	SX 2500	SX 2800			
Stratix 10 TX	TX 400	TX 850	TX 1100	TX 1650	TX 2100	TX 2500	TX 2800				
Stratix 10 MX	MX 1650	MX 2100									
Stratix 10 DX	DX 1100	DX 2100	DX 2800								
Stratix 10 NX	NX 2100										
Stratix 10 AX	1SA28										
Cyclone 10 GX	10CX085	10CX105	10CX150	10CX220							